

German Patent No. 100 22 973 A1

Job No.: 7527-115079

Ref.: DE10022973A1

Translated from German by the McElroy Translation Company
800-531-9977 customerservice@mcelroytranslation.com

FEDERAL REPUBLIC OF GERMANY
GERMAN PATENT AND TRADEMARK OFFICE
PATENT NO. 100 22 973 A1
(Offenlegungsschrift)

Int. Cl. ⁷ :	G 07 F 19/00 G 06 F 17/60
Filing No.:	100 22 973.5
Filing Date:	May 11, 2000
Domestic Priority	
Date:	June 15, 1999
No.:	199 27 322.7
Date Laid-open to Public Inspection:	February 8, 2001

METHOD FOR HANDLING FINANCIAL TRANSACTIONS BY MEANS OF ELECTRONIC
TRANSMISSION MEDIA

Inventor:	Bert Weingarten 23669 Timmendorfer Strand, DE
Applicant:	PAN AMP GmbH 22453 Hamburg, DE
Agent:	Eisenführ, Speiser & Partner 28195 Bremen

Examination request as per Art. 44 Patent Law has been filed.

The present method and system serves for handling electronic commerce. Credit card systems and systems based on credit cards represent the most common electronic payment systems. They are based on the transfer of credit card information to the seller, who then can collect the amount from the credit card company, without requiring the signature of the buyer. However, the credit card numbers are sometimes passed along the internet unencrypted. The disadvantages associated with the credit card system are self-evident, namely that there is no satisfactory protection against misuse, loss, falsification and multiple usage, and that furthermore, the anonymity of the consumer is not assured. It is therefore desirable to simplify and improve a method and a system for handling an electronic transaction. The invention is based on the idea that a subscriber 1, identified on the basis of an identification code, dials in to a primary server 3 and a sales server 4. The subscriber 1 selects a product offered on the sales

server 4. Next, the sales server 4 transmits the purchase price of the selected product to the subscriber 1 and to the primary server 3. A credit framework for the subscriber 1 is determined at an external bank server 18 by means of an account server 9 in the primary server 3, based on the purchase price of the selected product and based on ...

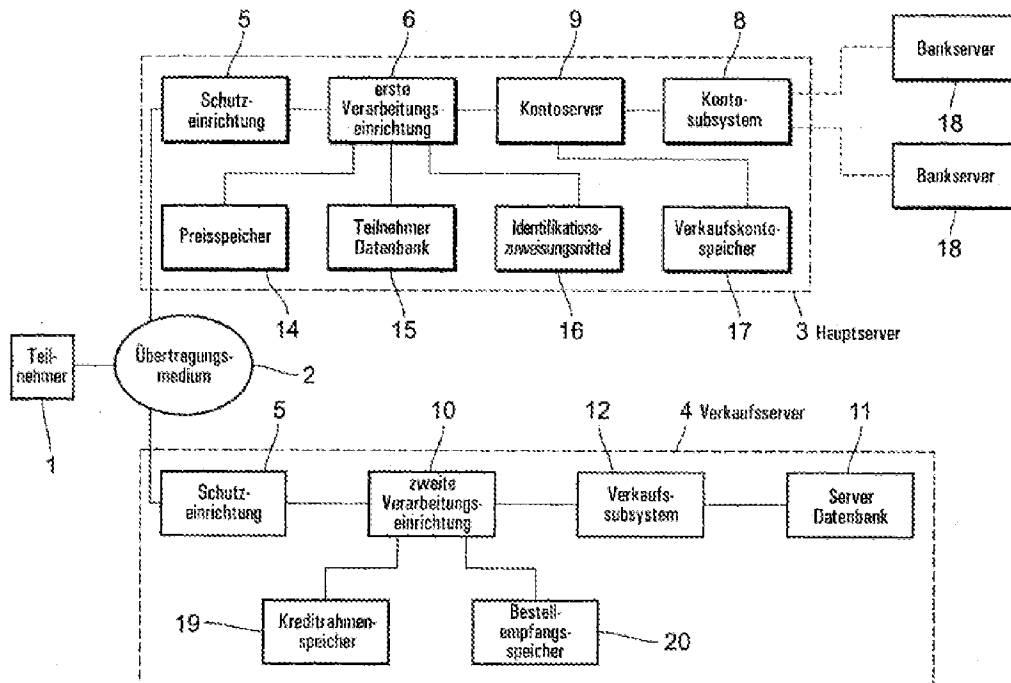


Fig. 1

- Key:
- 1 Subscriber
 - 2 Transfer medium
 - 3 Primary server
 - 4 Sales server
 - 5 Security device
 - 6 First processing device
 - 8 Accounting subsystem
 - 9 Account server
 - 10 Second processing device
 - 11 Server database
 - 12 Sales subsystem
 - 14 Price memory
 - 15 Subscriber database
 - 16 Identification allocation unit
 - 17 Sales account memory
 - 18 Bank server
 - 19 Credit framework memory
 - 20 Order reception memory

The following information has been taken from documentation submitted by the applicant.

Description

The present invention pertains to a method for handling of electronic commerce and to an associated electronic payment system.

The internet has been used heretofore primarily as an information exchange and advertising medium. Only recently are ever more software producers, service providers and banks setting up digital payment systems, especially in pilot projects. At the moment, the number of internet users is estimated to be about 40 million. The average subscriber no longer uses his computer only for text processing, but rather in addition to the communications function, increasingly also has discovered and made use of the commercial arm of the internet. In this case, the new electronic payment devices for electronic business, so-called E-commerce, have become quite important.

Electronic commerce opens up entirely new potentials, but also dangers, because the internet is an unsecured computer network. It is possible to listen in (intercept) data traffic (e.g., confidential data such as credit card numbers) or to impersonate another person without this being noted by the communications partner. Therefore, the consumer can only accept a method of electronic payment when it is assured that it is secure and that personal information will not get into unauthorized hands.

Furthermore, in principle the electronic payment device must enjoy acceptance by sellers and buyers and be suitable as a medium of exchange for non-physical goods, information and information services. In this case, the totality of a payment means, i.e., from penny amounts up to larger sums, must be covered.

Furthermore, the electronic payment device must be suitable for universal and international transactions for all internet subscribers in order to acquire products and services.

At this point in time, none of the existing formats has broken through and the payments are all handled by credit card companies.

Another important consideration in this regard is the anonymity of the consumer. The identity of the consumer must not be detectable from the electronic payment device; furthermore, information about the product purchases must not be accessible to third parties. This is intended to protect the privacy of the consumer, since information about transactions can allow information to be deduced about the purchasing and living circumstances of the consumer.

As mentioned above, credit card systems represent the most commonly used electronic payment systems. Credit card systems are based on the transfer of credit card information to the seller, who then can request the amount from the credit card company, without requiring the

signature of the buyer. However, credit card numbers are passed along the internet unencrypted. In addition, the buyer must be assured that he is sending his information to an authorized receiver, that is, the receiver must have been authorized by a credit card organization. The disadvantages associated with the credit card system are self-evident, namely that there is no satisfactory protection against misuse, loss, falsification and multiple usage, and that furthermore, the anonymity of the consumer is not assured.

A so-called cash-on-delivery system operates in the same manner as in a mail order business, but its complexity is still high. The costs per delivery at present amount to about 5 Euros. It is suitable only for physical products and the purchased articles must always be picked up at the post office.

An additional payment method is the Avant-card payment system. It is based on a Smart-Card technology and can be used in ordinary businesses, which have the equipment for reading the data. Avant is based on an embedded, integrated circuit that likewise has the necessary security modules. The buyer and the seller must have separate card readers and software. This system cannot be used internationally.

The so-called Solo/Kultaraha payment systems are based on financial transfers between the buyer and the seller, and both parties must be clients of the same bank. The service does not require any additional applications, but the bank must issue the needed user codes and passwords. Both systems can only be used for payments of more than 5 Euros.

In the known E-cash system, the consumer must open a customer account at a bank, with the consumer simultaneously receiving delivery of the needed software. Then the consumer deducts a particular amount from his account and transfers this amount digitally to his local computer. The money amount is stored as electronic funds with different values at the consumer's computer. Next, he can use these funds in order to purchase products/services/information from a vendor who accepts E-cash, or he can also transfer to or receive funds from other E-cash users. In this case the receiver of the electronic funds must likewise be a client of the same bank and maintain an E-cash account. However, this proves to be a disadvantage, since the E-cash user can only transfer and receive money within the E-cash union. Furthermore, the E-cash system has the disadvantage that the electronic or digital funds are not globally available when the computer is switched off or has a malfunction.

The SET system (Secure Electronic Transactions) represents an improvement to the credit card system. This system is a public standard for a secure credit card payment along nonsecure networks. In this case, the credit card information with a symmetrical 56-bit encryption is encoded together with the public 1024-bit encryption of the receiver. The information of the SET system is always provided with a digital fingerprint before sending; this fingerprint is encoded with the private key of the sender. Then the receiver can check by means

of the public key of the sender whether the information actually originates from it. In the case of payments with the SET system, encrypted credit card information is also passed along with the order. Due to the use of the SET system, the data are indeed protected along their path from the consumer to the vendor, but it offers no protection for the data of the consumer by the vendor. Furthermore, the sale must have a value of at least 5 Euros and the consumer always needs a credit card. Therefore, neither very small payments can be handled, nor is the anonymity of the consumer ensured.

The invention is based on the problem of simplifying and improving a method and a system for handling of electronic commerce.

This problem is solved by a method according to Claim 1 and by a system according to Claim 6. The invention is based on the idea that a subscriber dials in to a primary server and a sales server. In this case, the subscriber is identified in the primary server based on an identification code. The subscriber selects one of the products offered by the sales server. Next, the sales server transmits the purchase price of the selected product to the subscriber and to the primary server. A credit framework for the subscriber is determined by an external bank server by means of an account server in the primary server, based on the purchase price of the selected product and based on the identification code of the subscriber. A credit enable code is passed from the external bank server to the primary server when a corresponding credit framework of the subscriber is available. This credit enable code is then passed along from the primary server to the sales server. Finally, the product is transferred to the subscriber and the transfer of the purchase price from the subscriber's account to an account of the seller is initiated.

The advantages attained by the invention consist in particular in that the method is user-friendly, in that the identification of the subscriber takes place without input of a code or a sequence of digits. Furthermore, the privacy of the consumer is assured, in that the system preserves the anonymity of the consumer, since only the bank or the credit company verifies the credit worthiness of the consumer.

Additional configurations of the invention are the subject of the dependent claims.

Embodiments of the invention are described subsequently with reference to the illustration.

Shown are:

Figure 1, a basic block diagram of the payment system, and

Figure 2, a basic illustration of the payment system.

Figures 1 and 2 each illustrate an electronic payment system according to the invention. The primary constituents of the payment system are a subscriber 1, a transmission medium 2, preferably the internet, a central primary server 3 and at least one sales server 4. The subscriber 1, the primary server 3 and the sales server 4, are each connected to each other by the internet 2.

The primary server 3 can also be connected to one or several bank servers 18. The primary server 3 has a security apparatus 5, a first processing device 6, an account server 9 and an accounting subsystem 8, which are connected in series in the sequence described above. The first processing apparatus 6 is furthermore connected to an identification assignment unit 16, a subscriber database 15 and a pricing memory 14. The account server 9 is connected to a sales account memory 17.

The sales server 4 has a security apparatus 5, a second processing apparatus 10, a sales subsystem 12 and a server database 11, which are likewise connected in series in the manner described above. The second processing apparatus 10 is furthermore connected to a credit framework memory 19 and an order reception memory 20.

The subscriber 1 dials in to the internet 2 and searches for the sales server 4 of a vendor. Once the subscriber 1 has dialed into the internet 2, an identification code specific to the subscriber 1 is passed automatically to the primary server. The identification code must first pass the security apparatus 5 in the primary server. The security apparatus 5 represents a so-called firewall that is used to protect the primary server 3 against external threats. The security apparatus 5 then passes the identification code along to the first processing apparatus 6 of the primary server 3. In the first processing apparatus 6, the identification code is compared with information saved in the subscriber database 15 and the subscriber 1 is identified based on this information.

The subscriber 1 can select among the vendor's products offered on the sales server 4. Next, the purchase price of the selected product is passed to the subscriber 1 and to the primary server 3. The price of the selected product in this case is saved in the price memory 14 in the primary server 3.

It is also possible for the identification of the subscriber by the primary server 3 to not occur immediately when the subscriber dials in to the internet 2, but rather for the identification to be initiated by the sales server 4.

Based on the purchase price of the selected product and of the identification code specific for the subscriber 1 saved in the pricing memory 14, the credit framework of the subscriber 1 is determined. The concept of the credit framework pertains to both the funds available to the subscriber in an account, and also to the credit limit of the subscriber at a bank. In the account server 9 the identity of the subscriber determined based on the identification code, and also the amount of the purchase price of the selected product are processed and are passed along by means of the accounting subsystem 8 to an external bank server 18 with a prompt to check the credit framework. In this case only the identity of the subscriber, but not the specific identification code, is passed to the external bank server 18. Only the primary server 3 can establish the relationship between the identity of the subscriber and the identification code

specific for the subscriber 1. If the subscriber has either a sufficient account balance available in his account or if the subscriber 1 has a sufficiently large credit limit, the external bank server 18 transmits a credit enable code to the primary server 3. This code is then passed from the primary server 3 to the sales server 4, where the credit framework is saved in the credit framework memory 19 according to the credit enable code. However, it must be considered that the credit enable code is only associated with the subscriber's identification code in the account server 9. The credit enable code can also be viewed as the payment certificate.

Once the sales server 4 has received the credit enable code with the associated identification code, the second processing apparatus 10 initiates the transfer of the selected product to the subscriber 1. This can be a request for a packet service, the transfer of data or the enabling of a code so that the subscriber can download information from the server's database.

As soon as the subscriber has received the product, it passes an acknowledgement to both the primary server 3 and also to the sales server 4. As soon as the first processing apparatus 6 of the primary server 3 receives this confirmation, it passes the corresponding information along to the account server 9, which triggers an amount corresponding to the purchase price to be deducted from the account of the subscriber 1 to an external bank server 18 and to be credited to an account of the vendor at an external bank server 18. In this case, the subscriber 1 and the vendor need not have set up their accounts at the same external bank server 18. Due to the use of the accounting subsystem 8, it makes no difference at which external bank servers 18 the accounts are set up. It is important merely that the particular account be known to the accounting subsystem 8 at the particular external bank server 18.

In addition, the primary server 3 has an identification allocation unit 16. A specific identification code is associated with each subscriber 1 in this identification allocation unit 16. This identification code can be assigned centrally to the subscriber, for example, upon his first dial in or log in. Only the subscriber 1 and the primary server 3 know the relationship between the identity of the subscriber and the associated identification code. During the communication between the primary server 3 and the external bank servers 18, the identity, that is, the name of the subscriber and perhaps also his account number, is used. In other words, the external bank servers 18 do not know which identification code belongs to the identity of the subscriber 1.

During the communication between the primary server 3 and the sales server 4 on the other hand, only the specific identification code of the subscriber 1 is used. This means that the sales server 4 only knows the identification code, but not the identity of the subscriber.

The method for handling the electronic commerce is implemented in a client-server structure. In this case, one embodiment provides that this structure be implemented on a Java-based structure. Therefore, the subscriber is a Java client. Therefore, the method can be

used on all systems and platforms that support Java. As an example: Pocket organizer, Notebooks, Pen-computers, IBM compatible computers and Web television.

Furthermore, it is possible for the payment certificate or the credit enable code to be transmitted by means of short messages, also called SMS (Short Message Service) commonly used in the mobile GSM Standard.

The method and the system for handling the electronic commerce is suitable in particular for the sale of digital products, e.g., software on the internet, and these products can be music-graphic elements, multi-media products and texts.

In order to achieve a broad consumer acceptance, the subscriber need not input a password or a personal identification number at any point. The subscriber is automatically identified by the primary server 3 with the dial in to the internet 2. To increase the security of the transactions, an identification code can be assigned to each subscriber by the identification assignment unit 16 in the primary server 3. This code is maintained as above for identification of a subscriber 1 logged in to the internet. Furthermore, this identification code is used in the determination of the credit framework. Finally, the code is then used for the third time when one of the bank servers 18 passes a credit enable code to the primary server 3. As discussed above, this credit enable code or the payment certificate is associated with the identification code of the particular subscriber.

The method and the system for handling of electronic commerce makes possible very small payments. The payments can go down to as little as 0.00016 Euros. Furthermore, the payment basis can be differentiated, that is, a payment can be handled for a data file, a listing or for a time of usage.

Since the method is based on use of the internet, the method can be applied for all buyers of products. For example, the method can be saved on a central server, so that a user can download the information or data needed for this method.

The consumer and the vendor can maintain their bank accounts at different banking institutions, since a higher order account server 9 is used. This account server 9 acts as a connecting site between the individual banking institutions. Thus it is possible for the method to be in fact used on an international basis.

In summary, the problem underlying the invention, the good of the invention and also the idea for solving the problem are presented differently below.

More and more consumers and industries are buying and selling on the internet, which consequently means that E-commerce (electronic business) is increasing every year. At this moment, many users of the internet--buyers and sellers--are experiencing difficulties in the accounting and payment for products on the internet, which range from infringement on privacy to improper or even absence of payments by consumer and industry. If the European Community

wishes to increase the number of internet users, then it is very important that the accounting, the payment and the privacy of consumers be protected in a reliable manner. Unfortunately, the security of financial transactions on the internet currently has numerous deficiencies. In addition, the method of payment (e.g., with a credit card) is not safe from manipulation.

The inventors of the present application have recognized the problems mentioned above and have begun to work to solve these security problems. The objectives of the underlying project are therefore defined as follows:

To improve a financial security system for the global marketplace; to improve an E-payment concept with so-called 'digital coins'; to integrate the MSI (multi sentry implement)-system and E-payment into an overall new concept; to develop identification and authentication systems that guarantee the complete and total privacy of the user and to demonstrate this completely new concept on a practical basis.

In other words, it is a matter of developing a reliable and manipulation-proof method of payment and accounting on the internet.

The new system is aimed directly at the market for sales of digital products on the internet, which includes music, graphic elements, multimedia products, chips and text. In addition, the market is intended for non-digital products with the new possibilities for accounting and payment on the internet. In order to promote a broad consumer acceptance, the system is free of encumbrances for all users. The software is available for downloading from the internet throughout the entire world. Profits are generated from licensing fees from vendors of digital products.

The new system is based on: a different, user-friendly philosophy (KISS), wherein existing solutions and technologies are used to make E-payment processes simple and anonymous for consumer and vendor and independent of banks. The new system cannot be compared to an existing payment method.

The security of the system is achieved by means of codes that have to be used at three different points. If a computer hacker decodes the code, for example, at the bank, the system recognizes this and shuts down. In this manner it is impossible to penetrate into the system. This means that the system is 100% manipulation resistant and is highly reliable.

The software for use of the system can be downloaded from the internet. This means that the use of the system is possible for all purchasers of products. Also, the fact that the user does not have to remember a code or a number underscores the user-friendly features of the system. In addition, the system does not require any fee from the client. This accelerates acceptance of the new system among consumers and purchasers of (digital) products.

Consumers are identified automatically by the system due to the use of individual codes. This means that an unauthorized recording and disclosure of data is prevented.

The system guarantees 100% anonymity of the consumer to potential vendors. Only the bank or credit card company checks the credit-worthiness of the consumer

The system runs on JAVA software. This kind of software can be used in many different areas. For example:

To ensure that CDs, music etc. cannot be duplicated; to ensure that software cannot be duplicated. This means that software firms will have more control over the users of software.

Possibilities for E-commerce:

All goods and services offered on the internet can be acquired and paid for in a secure manner. Telecommunications potentials: The software can be used in the GSM.

The digital coins can be used globally since the money is always available in the bank account of the consumer or seller. This means that the money is shielded by the secure dial up and secure handling of the system. In this new system, digital coins are always active, digital coins.

The system of the present invention makes it possible to handle very small payments. These payments can go down to 0.00016 Euros. In addition, the payment basis can be differentiated: Data file, listing and usage time payments.

In several known payment systems, the purchaser and the seller must be clients of the same bank. In the system according to the present invention, the seller and buyer can have different banks.

Claims

1. Method for handling of electronic business, with the steps of:
 - selection of the subscriber (1) in a primary server (3) and a sales server (4),
 - identification of the subscriber (1) in the primary server (3) based on an identification code specific to the subscriber (1),
 - selection by the subscriber (1) of a product offered by the sales server (4),
 - transmittal of the purchase price of the selected product to the subscriber (1) and the primary server (3) by the sales server (4),
 - determination of a credit framework of the subscriber (1) based on his identification code due to an account server (8) contained in the primary server (3) at an external bank server (18) with regard to the purchase price of the selected product,
 - transmittal of a credit enable code from the external bank server (18) to the primary server (3) for the corresponding existing credit framework and transmittal of this code to the sales server (4), and
 - transfer of the product to the subscriber (1) and initiation of the transfer of the purchase price from the subscriber's (1) account to an account of the seller.

2. Method according to Claim 1, characterized in that the product is transferred after the sales server (4) has received the credit enable code.

3. Method according to Claim 1 or 2, characterized in that the identification code is assigned to the subscriber centrally from the primary server (3), so that only the primary server (3) will know the identity of the subscriber.

4. Method according to one of the preceding claims, characterized in that the subscriber (1) after receipt of the product, sends an associated report to the primary server (3), whereupon the latter initiates the transfer of the purchase amount from the subscriber's (1) account to an account of the seller.

5. Method according to one of the preceding claims, characterized in that the primary server (3) and the sales server (4) are also designed to administer and exchange even very small monetary amounts.

6. Electronic payment system, in particular to implement the method according to Claim 1, with at least one subscriber (1) to dial into a primary server (3) and into a sales server (4), a central, primary server (3) to identify the subscriber (1) based on an identification code specific to the subscriber (1), to determine a credit framework for the subscriber (1) based on his identification code with respect to the purchase price of a product selected from the offering of a sales server (4), for transmittal of a credit enable code received from an external bank server (18) corresponding to the credit framework of the subscriber (1), and to trigger the transfer of the purchase price from a subscriber's (1) account to an account of the seller, and

at least one sales server (4) for offering of products, for transmission of the purchase price of a product offered by the sales server and selected by the subscriber (1) to the primary server (3) and to the subscriber (1), for receiving of the credit enable code corresponding to the credit framework of the subscriber and to trigger the transfer of the product to the subscriber (1).

7. System according to Claim 6, characterized in that the sales server (4) triggers the forwarding of the product after receipt of the credit enable code from the primary server (3).

8. Server in particular for use as primary server in the method according to Claim 1, with a processing device (6) for checking of the identification code of a subscriber (1) based on saved subscriber data,

an account server (9) to receive price information about products selected by the subscriber that are offered by a sales server (4), and for determining of a credit framework of a subscriber based on the sales price of the product, and

- an accounting subsystem (8) for transfer of a money amount corresponding to the purchase price from the subscriber's (1) account to an account of the seller.

9. Server according to Claim 8, characterized in that the identification code is assigned to the subscriber (1) centrally from the primary server (3), so that only the primary server (3) knows the identity of the subscriber.

10. Server according to one of Claims 8 or 9, characterized in that the particular server (3, 4) is designed to administer and exchange even very small monetary amounts.

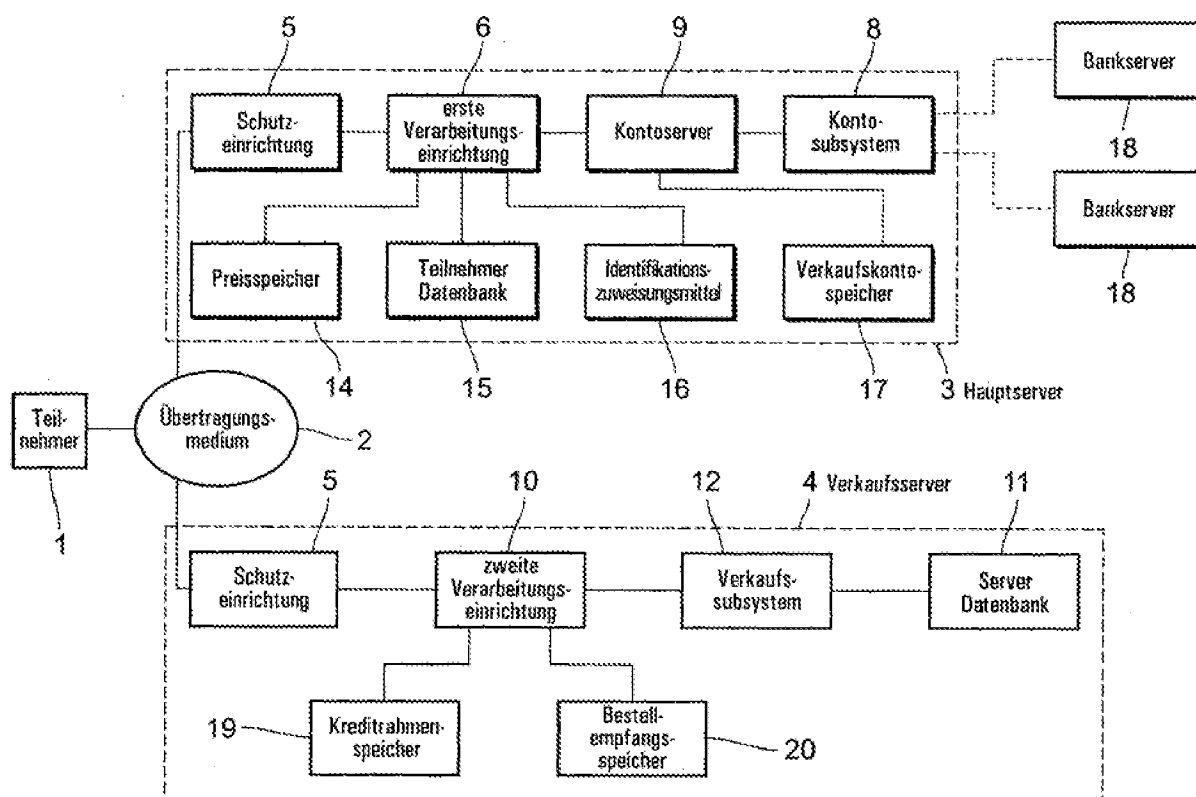
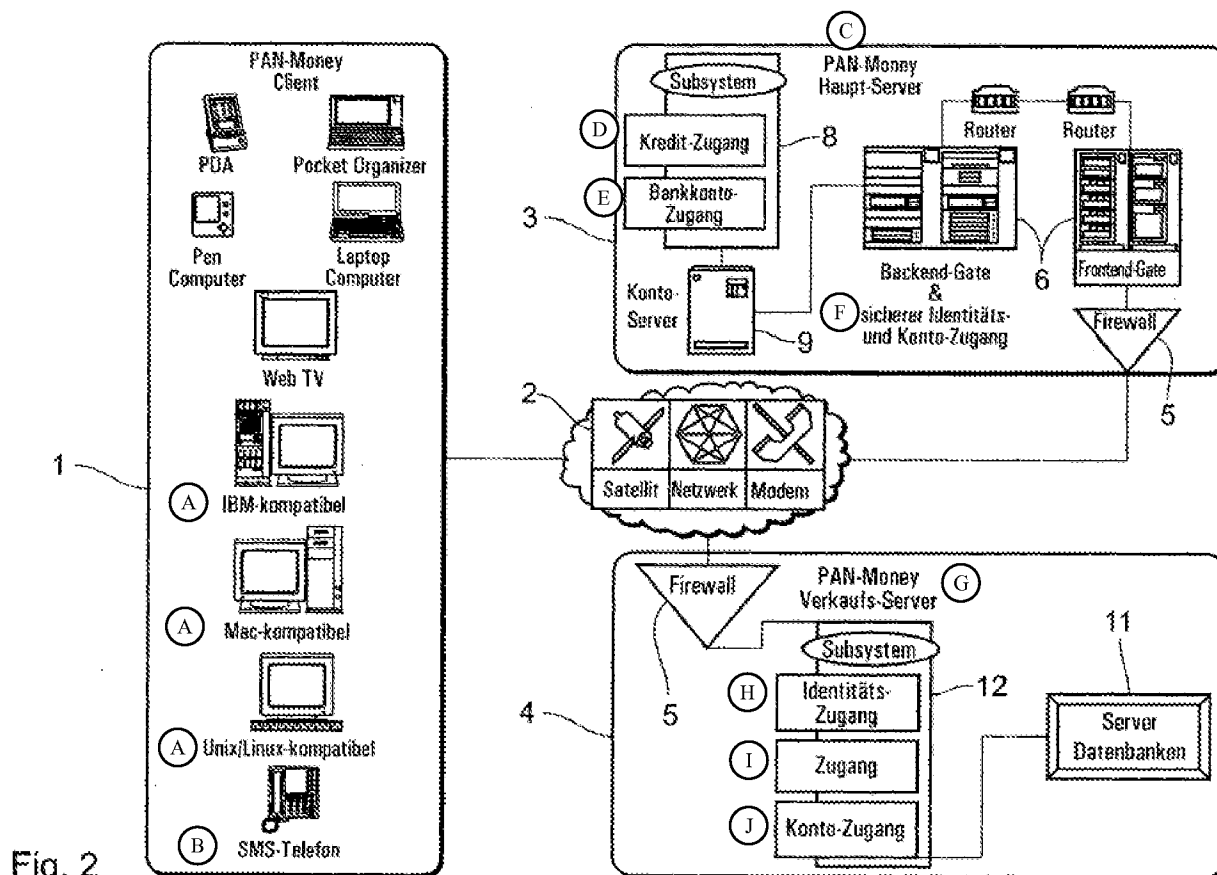


Fig. 1

- Key:
- 1 Subscriber
 - 2 Transfer medium
 - 3 Primary server
 - 4 Sales server
 - 5 Security device
 - 6 First processing device
 - 8 Accounting subsystem
 - 9 Account server
 - 10 Second processing device
 - 11 Server database
 - 12 Sales subsystem
 - 14 Price memory
 - 15 Subscriber database
 - 16 Identification allocation unit

- 17 Sales account memory
- 18 Bank server
- 19 Credit framework memory
- 20 Order reception memory



- Key:
- A Compatible
 - B Telephone
 - C Primary server
 - D Credit access
 - E Bank account access
 - F Secure identity and account access
 - G Sales server
 - H Access to identity
 - I Access
 - J Account access
 - 2 Satellite
 - 9 Account server
 - 11 Server databases